631 F.3d 266
United States Court of Appeals,
Sixth Circuit.

UNITED STATES of America, Plaintiff–Appellee,
v.
Steven WARSHAK (08–3997/4085; 09–3176); Harriet Warshak (08–3997/4087/4429); TCI Media, Inc. (08–3997/4212), Defendants–Appellants.

Nos. 08–3997, 08–4085, 08–4087, 08–4212, 08–4429, 09–3176. | Argued: June 16, 2010. | Decided and Filed: Dec. 14, 2010. | Rehearing and Rehearing En Banc Denied March 7, 2011.

BOGGS, Circuit Judge.

Berkeley Premium Nutraceuticals, Inc., was an incredibly profitable company that served as the distributor of Enzyte, an herbal supplement purported to enhance male sexual performance. In this appeal, defendants Steven Warshak ("Warshak"), Harriet Warshak ("Harriet"), and TCI Media, Inc. ("TCI"), challenge their convictions stemming from a massive scheme to defraud Berkeley's customers. Warshak and Harriet also challenge their sentences, as well as two forfeiture judgments.

Given the volume and complexity of the issues presented, we provide the following summary of our holdings:

(1) Warshak enjoyed a reasonable expectation of privacy in his emails vis-a-vis NuVox, his Internet Service Provider. *See Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). Thus, government agents violated his Fourth Amendment rights by compelling NuVox to turn over the emails without first obtaining a warrant based on probable cause. However, because the agents relied in good faith on provisions of the Stored Communications Act, the exclusionary rule does not apply in this instance. *See Illinois v. Krull,* 480 U.S. 340, 107 S.Ct. 1160, 94 L.Ed.2d 364 (1987).

* * *

*276 I. STATEMENT OF THE FACTS

A. Factual Background

In 2001, Steven Warshak ("Warshak") owned and operated a number of small businesses in the Cincinnati area. One of his businesses was TCI Media, Inc. ("TCI"), which sold advertisements in sporting venues. Warshak also owned a handful of companies that offered a modest line of so-called "nutraceuticals," or herbal supplements.[1] While the companies bore different names and sold different products, they appear to have been run as a single business, and they were later aggregated to form Berkeley Premium

Nutraceuticals, Inc. ("Berkeley"). In Berkeley's early days, the company's workforce was relatively minute; the company employed approximately 12 to 15 people, nearly all of whom were Warshak's friends and family. Among them was his mother, Harriet Warshak ("Harriet"), who processed credit-card payments.

* * *

In the latter half of 2001, Berkeley launched Enzyte, its flagship product. At the time of its launch, Enzyte was purported to increase the size of a man's erection. The product proved tremendously popular, and business rose sharply. By 2004, demand for Berkeley's products had grown so dramatically that the company employed 1500 people, and the call center remained open throughout the night, taking orders at breakneck speed. Berkeley's line of supplements also expanded, ballooning from approximately four products to around thirteen. By year's end, Berkeley's annual sales topped out at around $250 million, largely on the strength of Enzyte.

* * *

The popularity of Enzyte appears to have been due in large part to Berkeley's aggressive advertising campaigns. The vast majority of the advertising—approximately 98%—was conducted through television spots. Around 2004, network television was saturated with Enzyte advertisements featuring a character called "Smilin' Bob," whose trademark exaggerated smile was presumably the result of Enzyte's efficacy. The "Smilin' Bob" commercials were rife with innuendo and implied that users of Enzyte would become the envy of the neighborhood.

[The businesses engaged in a number of unlawful commercial practices, including cooking up advertising claims, hooking customers with a negative-option scheme, and lying to payment card processing services. Warshak personally directed much of the misconduct.]

* * *

B. Procedural History

In September 2006, a grand jury sitting in the Southern District of Ohio returned a 112–count indictment charging Warshak, Harriet, TCI, and several others with various crimes related to Berkeley's business. * * *

Before trial, numerous motions were filed. First, Warshak moved to exclude thousands of emails that the government obtained from his Internet Service Providers. That motion was denied. * * *

* * *

II. ANALYSIS

A. The Search & Seizure of Warshak's Emails

Warshak argues that the government's warrantless, *ex parte* seizure of approximately 27,000 of his private emails constituted a violation of the Fourth Amendment's prohibition on unreasonable searches and seizures. The government counters that, even if government agents violated the Fourth Amendment in obtaining the emails, they relied in good faith on the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701 et seq., a statute that allows the government to obtain certain electronic communications without procuring a warrant. The government also argues that any hypothetical Fourth Amendment violation was harmless. We find that the government *did* violate Warshak's Fourth Amendment rights by compelling his Internet Service Provider ("ISP") to turn over the contents of his emails. However, we agree that agents relied on the SCA in good faith, and therefore hold that reversal is unwarranted.[13]

1. *The Stored Communications Act*

The Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701 et seq., "permits a 'governmental entity' to compel a service provider to disclose the contents of [electronic] communications in certain circumstances." *Warshak II,* 532 F.3d at 523. As this court explained in *Warshak II:*

* * *

> The government may obtain the contents of e-mails that are "in electronic storage" with an electronic communication service for 180 days or less "only pursuant to a warrant." 18 U.S.C. § 2703(a). The government has three options for obtaining communications stored with a remote computing service and communications that have been in electronic storage with an electronic service provider for more than 180 days: (1) obtain a warrant; (2) use an administrative subpoena; or (3) obtain a court order under § 2703(d). *Id.* § 2703(a), (b).

532 F.3d at 523–24 (some alterations in original).

2. *Factual Background*

Email was a critical form of communication among Berkeley personnel. As a consequence, Warshak had a number of email accounts with various ISPs, including an account with NuVox Communications. In October 2004, the government formally requested that NuVox prospectively preserve the contents of any emails to or from Warshak's email account. The request was made pursuant to 18 U.S.C. § 2703(f) and it instructed NuVox to preserve all future messages.[14] NuVox acceded to the government's request and began preserving copies of Warshak's incoming and outgoing emails—copies that would not have existed absent the prospective preservation request. Per the government's instructions, Warshak was not informed that his messages were being

archived.

In January 2005, the government obtained a subpoena under § 2703(b) and compelled NuVox to turn over the emails that it had begun preserving the previous year. In May 2005, the government served NuVox with an *ex parte* court order under § 2703(d) that required NuVox to surrender any additional email messages in Warshak's account. In all, the government compelled NuVox to reveal the contents of approximately 27,000 emails. Warshak did not receive notice of either the subpoena or the order until May 2006.

3. *The Fourth Amendment*

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause...." U.S. CONST. amend. IV. The fundamental purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by government officials." *Camara v. Mun. Ct.,* 387 U.S. 523, 528, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967); *see Skinner v. Ry. Labor Execs.' Ass'n,* 489 U.S. 602, 613–14, 109 S.Ct. 1402, 103 L.Ed.2d 639 (1989) ("The [Fourth] Amendment ***284** guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government or those acting at their direction.").

Not all government actions are invasive enough to implicate the Fourth Amendment. "The Fourth Amendment's protections hinge on the occurrence of a 'search,' a legal term of art whose history is riddled with complexity." *Widgren v. Maple Grove Twp.,* 429 F.3d 575, 578 (6th Cir.2005). A "search" occurs when the government infringes upon "an expectation of privacy that society is prepared to consider reasonable." *United States v. Jacobsen,* 466 U.S. 109, 113, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984). This standard breaks down into two discrete inquiries: "first, has the [target of the investigation] manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?" *California v. Ciraolo,* 476 U.S. 207, 211, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986) (citing *Smith v. Maryland,* 442 U.S. 735, 740, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979)).

Turning first to the subjective component of the test, we find that Warshak plainly manifested an expectation that his emails would be shielded from outside scrutiny. As he notes in his brief, his "entire business and personal life was contained within the ... emails seized." Appellant's Br. at 39–40. Given the often sensitive and sometimes damning substance of his emails,[15] we think it highly unlikely that Warshak expected them to be made public, for people seldom unfurl their dirty laundry in plain view. *See, e.g., United States v. Maxwell,* 45 M.J. 406, 417 (C.A.A.F.1996) ("[T]he tenor and content of e-mail conversations between appellant and his correspondent, 'Launchboy,' reveal a[n] ... expectation that the conversations were private."). Therefore, we conclude that Warshak

had a subjective expectation of privacy in the contents of his emails.

The next question is whether society is prepared to recognize that expectation as reasonable. *See Smith,* 442 U.S. at 740, 99 S.Ct. 2577. This question is one of grave import and enduring consequence, given the prominent role that email has assumed in modern communication. *Cf. Katz,* 389 U.S. at 352, 88 S.Ct. 507 (suggesting that the Constitution must be read to account for "the vital role that the public telephone has come to play in private communication"). Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, "account" is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities. Much hinges, therefore, on whether the government is permitted to request that a commercial ISP turn over the contents of a subscriber's emails without triggering the machinery of the Fourth Amendment.

***285** In confronting this question, we take note of two bedrock principles. First, the very fact that information is being passed through a communications network is a paramount Fourth Amendment consideration. *See ibid.*; *United States v. U.S. Dist. Court,* 407 U.S. 297, 313, 92 S.Ct. 2125, 32 L.Ed.2d 752 (1972) ("[T]he broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."). Second, the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish. *See Kyllo v. United States,* 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (noting that evolving technology must not be permitted to "erode the privacy guaranteed by the Fourth Amendment"); *see also* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach,* 62 Stan. L.Rev. 1005, 1007 (2010) (arguing that "the differences between the facts of physical space and the facts of the Internet require courts to identify new Fourth Amendment distinctions to maintain the function of Fourth Amendment rules in an online environment").

With those principles in mind, we begin our analysis by considering the manner in which the Fourth Amendment protects traditional forms of communication. In *Katz,* the Supreme Court was asked to determine how the Fourth Amendment applied in the context of the telephone. There, government agents had affixed an electronic listening device to the exterior of a public phone booth, and had used the device to intercept and record several phone conversations. *See* 389 U.S. at 348, 88 S.Ct. 507. The Supreme Court held that this constituted a search under the Fourth Amendment, *see id.* at 353, 88

S.Ct. 507, notwithstanding the fact that the telephone company had the capacity to monitor and record the calls, *see Smith,* 442 U.S. at 746–47, 99 S.Ct. 2577 (Stewart, J., dissenting). In the eyes of the Court, the caller was "surely entitled to assume that the words he utter[ed] into the mouthpiece w[ould] not be broadcast to the world." *Katz,* 389 U.S. at 352, 88 S.Ct. 507. The Court's holding in *Katz* has since come to stand for the broad proposition that, in many contexts, the government infringes a reasonable expectation of privacy when it surreptitiously intercepts a telephone call through electronic means. *Smith,* 442 U.S. at 746, 99 S.Ct. 2577 (Stewart, J., dissenting) ("[S]ince *Katz,* it has been abundantly clear that telephone conversations are fully protected by the Fourth and Fourteenth Amendments.").

Letters receive similar protection. *See Jacobsen,* 466 U.S. at 114, 104 S.Ct. 1652 ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy [.]"); *Ex Parte Jackson,* 96 U.S. 727, 733, 24 L.Ed. 877 (1877). While a letter is in the mail, the police may not intercept it and examine its contents unless they first obtain a warrant based on probable cause. *Ibid.* This is true despite the fact that sealed letters are handed over to perhaps dozens of mail carriers, any one of whom could tear open the thin paper envelopes that separate the private words from the world outside. Put another way, trusting a letter to an intermediary does not necessarily defeat a reasonable expectation that the letter will remain private. *See Katz,* 389 U.S. at 351, 88 S.Ct. 507 ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

Given the fundamental similarities between email and traditional forms of communication, it would defy common sense ***286** to afford emails lesser Fourth Amendment protection. *See* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E–Mail,* 2008 U. Chi. Legal F. 121, 135 (2008) (recognizing the need to "eliminate the strangely disparate treatment of mailed and telephonic communications on the one hand and electronic communications on the other"); *City of Ontario v. Quon,* 560U.S. 746, 130 S.Ct. 2619, 2631, 177 L.Ed.2d 216 (2010) (implying that "a search of [an individual's] personal e-mail account" would be just as intrusive as "a wiretap on his home phone line"); *United States v. Forrester,* 512 F.3d 500, 511 (9th Cir.2008) (holding that "[t]he privacy interests in [mail and email] are identical"). Email is the technological scion of tangible mail, and it plays an indispensable part in the Information Age. Over the last decade, email has become "so pervasive that some persons may consider [it] to be [an] essential means or necessary instrument[ ] for self-expression, even self-identification." *Quon,* 130 S.Ct. at 2630. It follows that email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve. *See U.S. Dist. Court,* 407 U.S. at 313, 92 S.Ct. 2125; *United States v. Waller,* 581 F.2d 585, 587 (6th Cir.1978) (noting the Fourth Amendment's role in protecting "private communications"). As some forms of communication begin to diminish, the Fourth Amendment must recognize and protect

nascent ones that arise. *See Warshak I,* 490 F.3d at 473 ("It goes without saying that like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past.").

If we accept that an email is analogous to a letter or a phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment. An ISP is the intermediary that makes email communication possible. Emails must pass through an ISP's servers to reach their intended recipient. Thus, the ISP is the functional equivalent of a post office or a telephone company. As we have discussed above, the police may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call—unless they get a warrant, that is. *See Jacobsen,* 466 U.S. at 114, 104 S.Ct. 1652; *Katz,* 389 U.S. at 353, 88 S.Ct. 507. It only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception.

In *Warshak I,* the government argued that this conclusion was improper, pointing to the fact that NuVox contractually reserved the right to access Warshak's emails for certain purposes. While we acknowledge that a subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account, *see Warshak I,* 490 F.3d at 473; *Warshak II,* 532 F.3d at 526–27, we doubt that will be the case in most situations, and it is certainly not the case here.

As an initial matter, it must be observed that the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy. ***287** In *Katz,* the Supreme Court found it reasonable to expect privacy during a telephone call despite the ability of an operator to listen in. *See Smith,* 442 U.S. at 746–47, 99 S.Ct. 2577 (Stewart, J., dissenting). Similarly, the ability of a rogue mail handler to rip open a letter does not make it unreasonable to assume that sealed mail will remain private on its journey across the country. Therefore, the threat or possibility of access is not decisive when it comes to the reasonableness of an expectation of privacy.

Nor is the *right* of access. As the Electronic Frontier Foundation points out in its *amicus* brief, at the time *Katz* was decided, telephone companies had a right to monitor calls in certain situations. Specifically, telephone companies could listen in when reasonably necessary to "protect themselves and their properties against the improper and illegal use of their facilities." *Bubis v. United States,* 384 F.2d 643, 648 (9th Cir.1967). In this case, the NuVox subscriber agreement tracks that language, indicating that "NuVox *may*

access and use individual Subscriber information in the operation of the Service and as necessary to protect the Service." Acceptable Use Policy, *available at* http://business.windstream.com/Legal/acceptableUse.htm (last visited Aug. 12, 2010). Thus, under *Katz,* the degree of access granted to NuVox does not diminish the reasonableness of Warshak's trust in the privacy of his emails.[16]

Our conclusion finds additional support in the application of Fourth Amendment doctrine to rented space. Hotel guests, for example, have a reasonable expectation of privacy in their rooms. *See United States v. Allen,* 106 F.3d 695, 699 (6th Cir.1997). This is so even though maids routinely enter hotel rooms to replace the towels and tidy the furniture. Similarly, tenants have a legitimate expectation of privacy in their apartments. *See United States v. Washington,* 573 F.3d 279, 284 (6th Cir.2009). That expectation persists, regardless of the incursions of handymen to fix leaky faucets. Consequently, we are convinced that some degree of routine access is hardly dispositive with respect to the privacy question.

Again, however, we are unwilling to hold that a subscriber agreement will *never* be broad enough to snuff out a reasonable expectation of privacy. As the panel noted in *Warshak I,* if the ISP expresses an intention to "audit, inspect, and monitor" its subscriber's emails, that might be enough to render an expectation of privacy unreasonable. *See* 490 F.3d at 472–73 (quoting *United States v. Simons,* 206 F.3d 392, 398 (4th Cir.2000)). But where, as here, there is no such statement, the ISP's "control over the [emails] and ability to access them under certain limited circumstances will not be enough to overcome an expectation of privacy." *Id.* at 473.

We recognize that our conclusion may be attacked in light of the Supreme Court's decision in *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). In *Miller,* the Supreme Court held that a bank depositor does not have a reasonable expectation of privacy in the contents of bank records, checks, and deposit slips. *Id.* at 442, 96 S.Ct. 1619. The Court's holding in *Miller* was based on the fact that bank documents, "including financial statements and deposit slips, contain ***288** only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Ibid.* The Court noted,

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.... [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Id. at 443, 96 S.Ct. 1619 (citations omitted).

But *Miller* is distinguishable. First, *Miller* involved simple business records, as opposed to the potentially unlimited variety of "confidential communications" at issue here. *See ibid.* Second, the bank depositor in *Miller* conveyed information to the bank so that the bank could put the information to use "in the ordinary course of business." *Ibid.* By contrast, Warshak received his emails through NuVox. NuVox was an *intermediary,* not the intended recipient of the emails. *See* Bellia & Freiwald, *Stored E–Mail,* 2008 U. Chi. Legal F. at 165 ("[W]e view the best analogy for this scenario as the cases in which a third party carries, transports, or stores property for another. In these cases, as in the stored e-mail case, the customer grants access to the ISP because it is essential to the customer's interests."). Thus, *Miller* is not controlling.

Accordingly, we hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails "that are stored with, or sent or received through, a commercial ISP." *Warshak I,* 490 F.3d at 473; *see Forrester,* 512 F.3d at 511 (suggesting that "[t]he contents [of email messages] may deserve Fourth Amendment protection"). The government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause. Therefore, because they did not obtain a warrant, the government agents violated the Fourth Amendment when they obtained the contents of Warshak's emails. Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.

4. *Good–Faith Reliance*

[The panel concludes that investigators acted with good-faith reliance upon ECPA, and therefore declines to apply the exclusionary rule.]

* * *

KEITH, Circuit Judge, concurring.

* * *

[T]here is a further wrongdoing that troubles me today. Specifically, the government's request that NuVox preserve Warshak's stored and future email communications without Warshak's knowledge and without a warrant pursuant to § 2703(f). Under § 2703(f), "[a] provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to *preserve* records and other evidence *in its possession* pending the issuance of a court order or other process." 18 U.S.C. § 2703(f) (emphasis added). This subsection was added to the SCA in 1996 in an effort to supplement law enforcement resources and security. The Antiterrorism Act of 1996, Pub.L. 104–132, 110 Stat. 1305. While added in a completely

different context from the creation of the statute, it is worthwhile to review the purpose of the statute as a whole when considering the meaning of this subsection.

* * *

The plain language of § 2703(f) permits only the preservation of emails in the service provider's possession at the time of the request, not the preservation of future emails.[2] Moreover, the Department of Justice, along with some theorists, emphasize that these requests "have no prospective effect." *See, e.g.,* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act,* 72 Geo. Wash. L.Rev. 1557, 1565 (2004); U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Chapter III, § G(1) (2009), *available at* http://www.cybercrime.gov/ssmanual/03ssma.html ("[Section] 2703(f) letters should not be used prospectively to order providers to preserve records not yet created. If agents want providers to record information about future electronic communications, they should comply with the [Wiretap Act and the Pen/Trap statute]."). I find this statutory interpretation persuasive.

Following NuVox's policy, the provider would have destroyed Warshak's old emails but for the government's request that they maintain all current and prospective emails for almost a year without Warshak's knowledge. In practice, the government used the statute as a means to monitor Warshak after the investigation started without his knowledge and without a warrant. Such a practice is no more than back-door wiretapping. I doubt that such actions, if contested directly in court, would withstand the muster of the Fourth Amendment. Email, much like telephone, provides individuals with a means to communicate in private. *See Warshak v. United States,* 490 F.3d 455, 469–70 (6th Cir.2007), *vacated,* 532 F.3d 521 (6th Cir.2008) (en banc). The government cannot use email collection as a means to monitor citizens without a warrant anymore than they can tap a telephone line to monitor citizens without a warrant.

* * *

Nevertheless, because ***336** the government's violation of the Fourth Amendment stems from the order and/or subpoena to obtain Warshak's email communications pursuant to § 2703(b) and (d), the government acted in good faith upon the statute. The fact that their policy likely exceeded the parameters of § 2703(f) is irrelevant to this analysis as they did not rely upon § 2703 as a whole in requesting the secret subpoena and order to obtain these emails. Accordingly, the majority was correct in holding that the evidence falls within the good faith exception to the exclusionary rule.

* * *

Footnotes

[1] The companies also sold a product called Keflex, which supposedly masked traces of drugs in one's urine.

[13] Though we may surely do so, we decline to limit our inquiry to the issue of good-faith reliance. *See Pearson v. Callahan,* 555 U.S. 223, 129 S.Ct. 808, 818, 172 L.Ed.2d 565 (2009). If every court confronted with a novel Fourth Amendment question were to skip directly to good faith, the government would be given *carte blanche* to violate constitutionally protected privacy rights, provided, of course, that a statute supposedly permits them to do so. The doctrine of good-faith reliance should not be a perpetual shield against the consequences of constitutional violations. In other words, if the exclusionary rule is to have any bite, courts must, from time to time, decide whether statutorily sanctioned conduct oversteps constitutional boundaries. *See id.* at 816 (noting that repeated avoidance of constitutional questions leads to "constitutional stagnation" (citing *Saucier v. Katz,* 533 U.S. 194, 201, 121 S.Ct. 2151, 150 L.Ed.2d 272 (2001))).

[14] Warshak appears to have accessed emails from his NuVox account via POP, or "Post Office Protocol." When POP is utilized, emails are downloaded to the user's personal computer and generally deleted from the ISP's server.

[15] In a number of the NuVox emails, Warshak discussed the creation of trusts for his children, as well as the possibility that his financial dealings would mislead FTC investigators.

[16] We note that the access granted to NuVox was also temporally limited, as Warshak's email account was configured to delete his emails from NuVox's servers as soon as he opened them on his personal computer. *See* Appellant's Br. at 28 ("NuVox did not even save copies of account holders' received emails once they had been opened and downloaded to the account holders' computers[.]").

[1] The SCA refers generally to Chapter 121 of Title 18 of the United States Code, including sections 2701 through 2712. It was enacted as part of the Electronic Communications Privacy Act of 1986, Pub.L. No. 99–508, 100 Stat. 1848 (1986).

[2] This plain reading of the statute differs from that expressed in the majority opinion. *See supra* fn. 21. Though lower courts have followed my understanding of the statute, analysis of this statute appears to be one of first impression before a circuit court. *See In re Application for Pen Register and Trap/Trace Device,* 396 F.Supp.2d 747, 760 (S.D.Tex.2005), *abrogated by In re United States for Historical Cell Site Data,* 747 F.Supp.2d 827 (S.D.Tex.2010) (noting that the SCA is retrospective in nature as opposed to the Wiretap Act); *In re Application for U.S. for an Order Authorizing Disclosure of*

Location Based Services, 2007 WL 2086663, *1 (S.D.Tex. July 6, 2007) (noting that nothing in § 2703 authorizes the Government to demand that a provider prospectively "create records which would not otherwise exist in the ordinary course of business"); *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device,* 396 F.Supp.2d 294, 313–14 (E.D.N.Y.2005) (concluding, based upon the language of § 2703 as a whole, that the statute "does *not* authorize a court to enter a prospective order to turn over data as it is captured" because of the retrospective nature of the statute).